

CLAIMS:

1 1. A method of automatically obtaining a second
2 certificate for a user using a first certificate, the method
3 comprising:
4 accessing a registration server using a user's
5 server and the first certificate of the user to create a
6 connection that authenticates both the user's server identity
7 via a server certificate of the user server and the user's
8 identity via the user's first certificate;
9 creating a secure data channel between the
10 registration server and the user server;
11 forwarding a request for the second certificate from
12 the user server to the registration server;
13 determining in the registration server that the user
14 is entitled to the second certificate;
15 forwarding a request from the registration server to
16 an authority to generate a private/public key pair;
17 sending the private key to the user from the
18 authority via the secure data channel;
19 sending the public key from the authority to another
20 authority to be signed; and
21 forwarding the second certificate from the another
22 authority to a directory.

1 2. The method of claim 1, further comprising sending a
2 backup copy of the private key from the authority to a key
3 recovery authority.

1 **3.** The method of claim **1**, wherein the first certificate
2 comprises a signature certificate.

1 **4.** The method of claim **1**, wherein the second
2 certificate comprises an encryption certificate.

1 **5.** The method of claim **1**, wherein the first certificate
2 comprises an expiring signature certificate and the second
3 certificate comprises a replacement signature certificate.

1 **6.** The method of claim **1**, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises a replacement encryption certificate.

1 7. The method of claim 1, wherein the first certificate
2 comprises a signature certificate and the second certificate
3 comprises one of either the user's current encryption
4 certificate or an expired encryption certificate of the user.

1 8. A method of automatically obtaining a second
2 certificate for a user using a first certificate, the method
3 comprising:
4 accessing a server platform using a user's server
5 and the first certificate of the user to create a connection
6 that authenticates both the user's server identity via a
7 server certificate of the user server and the user's identity
8 via the user's first certificate;

9 creating a secure data channel between the server
10 platform and the user server;

11 forwarding a request for the second certificate from
12 the user server to the server platform; and

13 generating at the server platform the second
14 certificate.

1 ⁹
2 ¹¹1. The method of claim 8, wherein the first certificate
3 comprises a signature certificate.

1 ¹⁰
2 ¹²2. The method of claim 8, wherein the second
3 certificate comprises an encryption certificate.

1 ¹¹
2 ¹³3. The method of claim 8, wherein the first certificate
3 comprises an expiring signature certificate and the second
4 certificate comprises a replacement signature certificate.

12/14. The method of claim 8, wherein the first certificate
 1 comprises a signature certificate and the second certificate
 2 comprises a replacement encryption certificate.
 3

13/15. The method of claim 8, wherein the first certificate
 1 comprises a signature certificate and the second certificate
 2 comprises one of either the user's current encryption
 3 certificate or an expired encryption certificate of the user.
 4

14/16. An apparatus for automatically obtaining a second
 1 certificate for a user using a first certificate, the
 2 apparatus comprising:
 3

4 a user server and a registration server, the user
 5 server accessing the registration server using the first
 6 certificate of the user to create a connection that
 7 authenticates both the user's server identity via a server
 8 certificate of the user server and the user's identity via the
 9 user's first certificate;

10 a secure data channel, the secure data channel being
 11 disposed between the registration server and the user server,
 12 the user server forwarding a request for the second
 13 certificate to the registration server through the secure data
 14 channel;

15 a first authority, the registration server
 16 determining that the user is entitled to the second

17 certificate and forwarding a request to the first authority to
18 generate a private/public key pair, the first authority
19 sending the private key to the user via the secure data
20 channel;

21 a second authority, the first authority sending the
22 public key to the second authority to be signed; and

23 a directory, the second authority forwarding the
24 second certificate to the directory.

1 ¹⁵~~14~~. The apparatus of claim ¹⁴~~16~~, wherein the first
2 certificate comprises a signature certificate.

1 ¹⁸~~17~~. The apparatus of claim ¹⁴~~16~~, wherein the second
2 certificate comprises an encryption certificate.

1 ¹⁷~~16~~. The apparatus of claim ¹⁴~~16~~, wherein the first
2 certificate comprises an expiring signature certificate and
3 the second certificate comprises a replacement signature
4 certificate.

1 ¹⁸~~20~~. The apparatus of claim ¹⁴~~16~~, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises a replacement encryption certificate.

1 ¹⁹/₂₁. The apparatus of claim ¹⁶/₁₄ wherein the first
 2 certificate comprises a signature certificate and the second
 3 certificate comprises one of the user's current encryption
 4 certificate and an expired encryption certificate of the user.

1 ²⁰/₂₄. An apparatus for automatically obtaining a second
 2 certificate for a user using a first certificate, the
 3 apparatus comprising:

4 a user server and a server platform, the user server
 5 accessing the server platform using the first certificate of
 6 the user to create a connection that authenticates both the
 7 user's server identity via a server certificate of the user
 8 server and the user's identity via the user's first
 9 certificate;

10 a secure data channel, the secure data channel being
 11 disposed between the server platform and the user server;

12 the user server forwarding a request for the second
 13 certificate to the server platform; and

14 the server platform generating the second
 15 certificate.

1 ²¹/₂₃. The apparatus of claim ²²/₂₀, wherein the first
 2 certificate comprises a signature certificate.

1 ²²₂₄. The apparatus of claim ²⁰₂₂, wherein the second
2 certificate comprises an encryption certificate.

1 ²³₂₅. The apparatus of claim ²⁰₂₂, wherein the first
2 certificate comprises an expiring signature certificate and
3 the second certificate comprises a replacement signature
4 certificate.

1 ²⁴₂₆. The apparatus of claim ²⁰₂₂, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises a replacement encryption certificate.

1 ²⁵₂₇. The apparatus of claim ²⁰₂₂, wherein the first
2 certificate comprises a signature certificate and the second
3 certificate comprises one of either the user's current
4 encryption certificate or an expired encryption certificate of
5 the user.

FILED
1/12/16
"OFFICE"